Computers, Materials & Continua
DOI:10.32604/cmc.2022.018589
Article

Tech Science Press

A Secure and Efficient Cluster-Based Authentication Scheme for Internet of Things (IoTs)

Kanwal Imran[1,*], Nasreen Anjum[2], Abdullah Alghamdi[3], Asadullah Shaikh[3], Mohammed Hamdi[3] and Saeed Mahfooz[1]

[1]Department of Computer Science, University of Peshawar, Peshawar, 25121, Pakistan
[2]Department of Informatics, King's College London, London, SE5 9RJ, UK
[3]College of Computer Science and Information Systems, Najran University, Najran, 61441, Saudi Arabia
[*]Corresponding Author: Kanwal Imran. Email: kanwalim@uop.edu.pk
Received: 13 March 2021; Accepted: 29 May 2021

Abstract: IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) provides IP connectivity to the highly constrained nodes in the Internet of Things (IoTs). 6LoWPAN allows nodes with limited battery power and storage capacity to carry IPv6 datagrams over the lossy and error-prone radio links offered by the IEEE 802.15.4 standard, thus acting as an adoption layer between the IPv6 protocol and IEEE 802.15.4 network. The data link layer of IEEE 802.15.4 in 6LoWPAN is based on AES (Advanced Encryption Standard), but the 6LoWPAN standard lacks and has omitted the security and privacy requirements at higher layers. The sensor nodes in 6LoWPAN can join the network without requiring the authentication procedure. Therefore, from security perspectives, 6LoWPAN is vulnerable to many attacks such as replay attack, Man-in-the-Middle attack, Impersonation attack, and Modification attack. This paper proposes a secure and efficient cluster-based authentication scheme (CBAS) for highly constrained sensor nodes in 6LoWPAN. In this approach, sensor nodes are organized into a cluster and communicate with the central network through a dedicated sensor node. The main objective of CBAS is to provide efficient and authentic communication among the 6LoWPAN nodes. To ensure the low signaling overhead during the registration, authentication, and handover procedures, we also introduce lightweight and efficient registration, de-registration, initial authentication, and handover procedures, when a sensor node or group of sensor nodes join or leave a cluster. Our security analysis shows that the proposed CBAS approach protects against various security attacks, including Identity Confidentiality attack, Modification attack, Replay attack, Man-in-the-middle attack, and Impersonation attack. Our simulation experiments show that CBAS has reduced the registration delay by 11%, handoff authentication delay by 32%, and signaling cost

by 37% compared to the SGMS (Secure Group Mobility Scheme) and LAMS (Light-Wight Authentication & Mobility Scheme).

Keywords: IoT; cyber security; security attacks; authentication delay; handover delay; signaling cost; 6LoWPAN

1 Introduction

The Internet of Things (IoTs) is the new complex network that is connecting billions of smart devices and enabling access to information "anytime" and "anywhere" and using "anything" and "anyone". The worldwide adoption of wireless technologies such as Wi-Fi, Bluetooth, and Zigbee has improved IoT infrastructure's scalability and has massively increased the number of connected devices. According to [1], the number of IoT devices worldwide are predicted to reach more than 25.4 billion in 2030. However, this results in limitations for the devices connected via the wireless communication links such as high cost, low battery power, high energy consumption, limited communication distance, limited IP addresses, and weak security [2–4].

New protocols, standards, and technologies have been adopted in IoTs to support the wireless nodes with limited and heterogeneous resources such as limited computation power, small storage capacity and, low battery power and interconnected via the lossy and error prone radio links [5,6]. For instance, based on the IPv6 and IEEE 802.15.4 standard the IETF (Internet Engineering Task Force) has developed a standard called 6LoWPAN (IPv6 over low Power Wireless Personal Area Networks) for highly constrained nodes interconnected via the lossy links. 6LoWPAN is the intermediate layer between the standard IPv6 and low power and lossy IEEE 802.15.4 wireless network [7,8]. The main objective of 6LoWPAN is to provide fast, efficient, and reliable connectivity to highly constrained nodes using the IPv6 protocol [9]. Many research studies claimed that 6LoWPAN is the ideal solution to provide the seamless and reliable connectivity to highly constrained sensor nodes in IoTs [10–13]. However, from the security perspective, 6LoWPAN requires a considerable attention from the research community. For instance, the data link layer of IEEE 802.15.4 in 6LoWPAN is based on AES (Advanced Encryption standard), but the 6LoWPAN standard lacks and has omitted the security and privacy requirements at higher levels such as secure and efficient authentication of sensor nodes [14–16]. The sensor nodes in 6LoWPAN can join the network without requiring the authentication procedure. Therefore, from security perspectives, 6LoWPAN is vulnerable to many attacks such as replay attack, Man-in-the-Middle attack, Impersonation attack, and Modification attack.

1.1 Related Work and Motivation

To resolve the authentication security issue of IP-based sensor nodes in 6LoWPAN, several authentication schemes have been proposed. For instance, the authors in [17] have proposed an authentication scheme which provides mutual authentication for M2M communication to achieve a secure transmission during the mobility in 6LoWPAN networks. The proposed scheme enables a 6LoWPAN sensor node to authenticate with the remote server by establishing session keys. However, the details of pairwise pre-distribution keys among the sensor nodes are missing in this paper. The authors in [18] proposed a secure admission control scheme for 6LoWPAN. The proposed solution includes node authorization, detection, authentication, and data filtering to discard data from the unauthorized nodes. It uses the cryptographic algorithm based on the AES symmetric key to isolate the nodes which are not authorized and eligible to connect with the legitimate nodes or network. The authors in [19] presented a secret key distribution and

detection method to provide resistance against the anti-capture attack. A secure group mobility scheme (SGMS) has been proposed in [20]. The SGMS ensures the handovers of multiple nodes simultaneously by using the cryptographic algorithms. However, this scheme involves extra signaling exchange among the nodes in 6LoWPAN, making this scheme less efficient. The authors in [21] proposed a lightweight authentication scheme for resource-constrained industrial devices in 6LoWPAN. Although the proposed solution offers low computation cost, it still has handover and signaling overhead.

1.2 Proposed Scheme and Contributions

Interestingly, all the above-mentioned authentication schemes have been proposed to authenticate a single node at a time. When a single sensor node joins a network; it must authenticate when it connects to a new domain which increases the handover latency and makes transmission slow and inefficient. Furthermore, single node authentication schemes require additional registration and authentication signals exchange among the AAA (Authentication, Authorization and Accounting), MAG (Mobile Access Gateway) and LMA (Local Mobility Anchor), which further increases the handoff latency and packet loss during the transmission.

Our proposed approach is designed to overcome the limitations in single node authentication schemes [17–21]. We propose a Secure Cluster-Based Authentication Scheme (CBAS) for 6LoWPAN based on the PMIPv6 (Proxy Mobile IPv6) developed by a working group NETLMM (Network-based localized mobility management) [22–24]. In contrast to [17–21], we propose to merge the functions of LMA and AAA into the MAG. Now the handover process is performed between two neighboring MAGs without going through the LMA, therefore reducing the signaling cost during the handover procedure. MAG is also responsible for the authentication and binding of a cluster of sensor nodes through the new entity we called Supervisory-Node. Furthermore, CBAS is based on lightweight cryptographic algorithms such as random numbers and hash function to provide the secure authentication to highly constrained mobile nodes in 6LoWPAN.

Our contributions in this article are summarized as follows:

- In this paper, a secure cluster-based authentication scheme for highly constrained sensor nodes in 6LoWPAN is proposed. The main objective of CBAS is to overcome the signaling overhead and ensures secure and efficient communication among the 6LoWPAN nodes during the registration and handover process. In this approach, sensor nodes are organized into a cluster and communicate with the MAG through a cluster leader; we call Supervisory-Node. The Supervisory-Node communicates with the MAG directly on behalf of the sensor nodes in the cluster.
- We also introduce a lightweight and secure registration, de-registration, and initial authentication and handover procedure when a sensor node joins or leaves a cluster. Our simulation experiments show that CBAS shows better performance in terms of low signaling cost during the registration and handover procedure compared to the state-of-the-art protocols.
- Our security analysis shows that the proposed CBAS approach protects against various security attacks, including Identity Confidentiality attack, Modification attack, Replay attack, Man-in-the-middle attack, and Impersonation attack. Our simulation experiments show that, CBAS shows better performance in terms of low signaling cost and low handover and authentication delay.

1.3 Paper Organization

The remainder of this article is organized as follows: Section 2 describes the proposed CBAS architecture. Section 2 presents the registration, de-registration, initial authentication, and handover procedures performed in CBAS. Section 3 discusses the performance of the CBAS scheme in terms of the handover authentication delay and signaling cost. Section 4 presents numerical results and security analysis. Section 5 finally concludes our research efforts.

2 Architecture of Cluster-Based Authentication Scheme (CBAS) in 6LoWPAN

The architecture of CBAS is shown in Fig. 1. The CBAS comprises three elements: (i) Host-Node, (ii) Supervisory-Node, and (iii) MAG.

2.1 Host-Node

The Host-Node is an RFD (Reduced functional device) that is responsible for gathering sensory data. This device is a highly constrained node (limited computational and battery power) and communicate with other nodes in the network over unreliable and lossy wireless links.

2.2 Supervisory-Node

The Supervisory-Node is a mobile, fully functional sensor device (FFD). In contrast to Host-Node, it possesses strong processing, battery, and storage resources. It is represented as FFD in Fig. 1. The FFD is selected based on its larger storage and computational resources. When multiple FFDs exist in a network, the FFD with a short distance from the base station is selected as a Supervisory-Node. The Supervisory-Node, as a vital element of the CBAS scheme, performs many essential functions and responsibilities. For instance,

It is responsible for creating and managing a cluster of Host-Nodes. It creates, controls, and manages a cluster through the registration and deregistration procedures. For secure registration and authentication to a cluster, it maintains and manages a table in its storage; we called it a Binding-Table. The Binding-Table stores the entry information of each Host-Node including, Host-Node id, cluster-id (the id of a cluster it belongs to), Host-Node's location, random numbers, and temporary identities (used to keep the node information safe from the malicious activities and attackers). The supervisory-node regularly updates the Binding-Table for various reasons. For example, when a Host-Node changes its location or switches to another cluster.[1]

- The supervisory-Node acts as a coordinator between the Host-Nodes and MAG. It routes the packets from the Host-Node to MAG. It controls the messages exchange between Host-Node and MAG for low signaling overhead and efficient communication. Additionally, it performs signaling control with the MAG on the behalf of other nodes of its cluster.

2.3 Mobile Access Gateway

The main purpose of the CBAS scheme is to provide secure authentication to Host-Nodes with low signaling overhead when they join a cluster. To achieve our objective, in comparison to the SGMS [20], in our proposed architecture, the functions and responsibilities of Local Mobility

[1] We assume that Host-Nodes evaluate their locations using the available positioning services such as GPS (General Positioning System) and send their location to Supervisory node whenever they change their location or switch to another cluster.

Anchor and Authentication, Authorization and Accounting server are merged into the MAG[2]. The handover operation is performed between two adjacent MAGs without the assistance of LMA. The MAG now directly exchanges its information with its neighboring MAGs without going through the LMA. Further, MAG does not have to perform the deregistration and binding update operation with the LMA. This enhancement to the existing architecture avoids the extra control message exchange among the MAG nodes. Thus, further leading to low signaling overhead and cost. The main functions and responsibilities of MAG in our proposed architecture are as follows:

- MAG is responsible for the selection and registration of Supervisory-Nodes based on their storage and computational resources.
- MAG is also responsible for the registration, secure authentication, and de-registration of Host-Nodes through the Supervisory-Nodes. To do so, MAG maintains and manages a table called MAG-Table. MAG uses its table to store and update the authentication and registration information of registered Host-Nodes and Supervisory-Nodes.
- MAG is also responsible for a secure handover when a Host-Node travels from one MAG to another MAG.

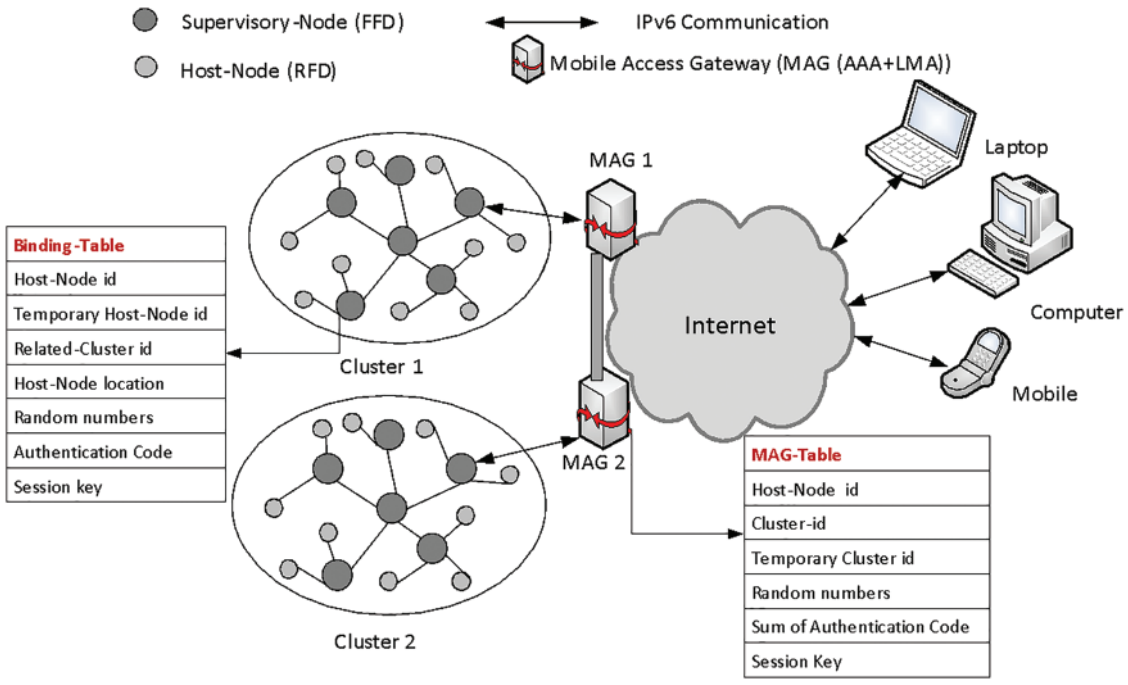

Figure 1: Architecture of CBAS in 6LoWPAN

3 Registration, De-registration, Initialization and Handover Procedures in (CBAS) for 6LoWPAN

In this section, we describe the registration, de-registration, authentication, and handover procedures. Tab. 1 shows the notations used in all the procedures.

[2] MAG is also known as 6LoWPAN gateway [24,25].

Table 1: Notations used in registration, de-registration, authentication, and handover procedures

Notations	Descriptions
Id	Host-node identity
tId	Temporary host-node identity
cId	Cluster identity
tcId	Temporary cluster identity
h	Hash function
R	Random number of host-node
hMsg	Hash-based message authentication code
Ky	Session key (establish between two Host-Nodes)
Ct	Ciphertext of host-node
Msg	Message authentication code
AC	Authentication code of host-node
AC_{sum}	Sum of authentication codes

3.1 Registration of a Host-Node with MAG through the Supervisory-Node

To join a cluster securely, a Host-Node needs to register with MAG through the Supervisory-Node. The registration procedure of a Host-Node with MAG through the Supervisory-Node is depicted in Fig. 2.

Step 1: At the beginning, the Binding-Table is empty. A Host-Node desires to register with a cluster, first initiates a broadcast call (initial-attachment). The initial-attachment message consists of unique identity of the Host-Node (Id) and R1 (random number). The random numbers are generated for a secure authentication purpose. We assume that the Host-Node, Supervisory-Node, and MAG generate the random number using the tineyRNG random number generation function [26][3] for a secure and authentic registration process.

Step 2: Upon receiving the registration request, the Supervisory-Node scans its Binding-Table to check whether the requested Host-Node is already registered or not. If yes, then Supervisory-Node denies the registration request and updates the location information. If no, then the Supervisory-Node will register the Host-Node by creating a new entry in the Binding-Table. The entry information of the registered Host-Node contains the Host-Node-id, Host-Node-location, and unidentifiable random number. After then, Supervisory-Node accumulates its cluster-id (cId) with a message and sends the updated information to the MAG.

Step 3: The MAG, upon receiving the update information request, scans its MAG-Table to check whether the Host-Node is already registered or not. If no, then MAG creates an entry for the Host-Node and sends back a registration response to the Supervisory-Node with a temporary identity (tId) and a random number R2.

Step 4. Then, Supervisory-Node sends a message with <tId, cId, R2> information to the Host-Node. The tId is then published by the Host-Node to the public. The reason is to keep the device information safe from the attackers and prevent attackers from tracking the Host-Node. The Host-Node, Supervisory-Node, and MAG store <Id, tId, cId, R1, R2> information in their tables, accordingly.

[3] TinyRNG is an efficient, secure, and undetectable Cryptographic Pseudo-Random Number Generator. It has been designed to minimize the memory usage and energy consumption of sensor nodes.

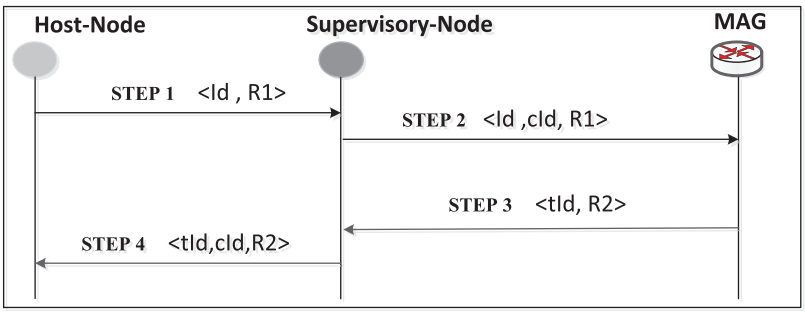

Figure 2: Registration procedure of Host-Nodes with MAG through the Supervisory-Nodes

3.2 De-registration Procedure of a Host-Node with MAG through the Supervisory-Node

In our proposed CBAS architecture, the de-registration process occurs when a Host-Node is not performing any activity in the network or when a Host-Node willingly wants to leave a cluster. In a case, if a Host-Node is not active for a long-time duration[4], its registration information will be removed from both Binging-Table and MAG-Table. In a case, a Host-Node willingly wants to leave the cluster, following steps will be performed. The De-registration procedure is shown in Fig. 3.

Step 1: The Host-Node sends a de-registration call to the Supervisory-Node.

Step 2: Upon receiving the deregistration request, the Supervisory-Node removes the registration information of the requested Host-Node from its Binding-Table and updates it.

Step 3: Then, Supervisory Node forwards the de-registration request of the Host-Node to the MAG.

Step 4: Now the MAG also removes the Host-Node from its MAG-Table and updates it.

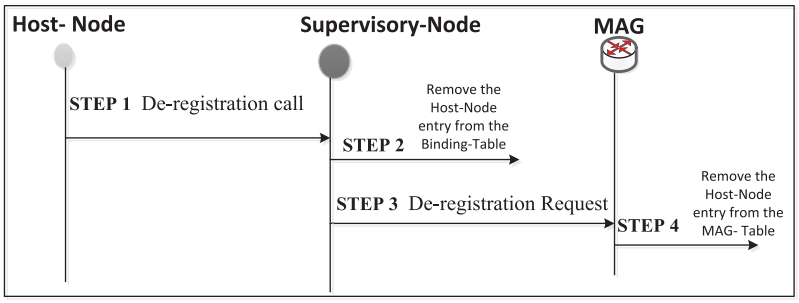

Figure 3: De-registration procedure of Host-Nodes with MAG through the supervisory-node

3.3 Initial Authentication Procedure

When a registered Host-Node joins the network after its registration with MAG through the Supervisory-Node, an initial authentication procedure with the MAG is needed. In this

[4] The time duration of the inactive node is decided based on its use cases. For instance, in a very active environment, the duration may last from hours to days. However, in a less active environment, the time duration may last from weeks to months."

procedure, Host-Node, Supervisory-Node and MAG exchange messages to achieve a mutual initial authentication and key establishment. The procedure of initial authentication is shown in Fig. 4.

Step 1: When a Host-Node or group of Host-Nodes join a cluster, they generate a message authentication code (Msg) based on the Hash function (ACi = $hACky_{HN-LD}$(tIdi, Idi, R2))[5]. Then, the generated authentication message <tIdi, ACi> is sent to the Supervisory-Node. After receiving the authentication message, Supervisory-Node integrates its own authentication information with the authentication message to form a MList. Then, Supervisory-Node calculates the sum of the message values ($AC_{sum} = AC_1 \oplus \ldots \oplus AC_N \oplus AC_{LD}$), and encrypts the sum of values and MList (MList = tId_1,.., tId_N, tId_{LD}) using a session key.

Step 2: The Supervisory-Node sends a router solicitation (RS) message (<tId_{LD}, $eky_{LD\text{-}MAG}$, AC_{sum}, Mlist) to the MAG. On getting the MList, MAG first derives the identity of each Host-Node to calculate Msg value and verifies the Msg value by comparing it with received Msg value. If the calculated Msg value and the received Msg value are different (Step 1), then MAG sends a message to the Host-Node and requests for detailed Msg values of each Host-Node. The main reason for this step is to investigate whether the Host-Node or group Host-Node are legal or not. If the information included in the Msg values is not correct, a warning message is sent to the Host-Node to inform about the illegitimacy of the devices. If the calculated Msg value matches the value of the received message, then MAG accepts the Host-Node as an authentic node to join the cluster.

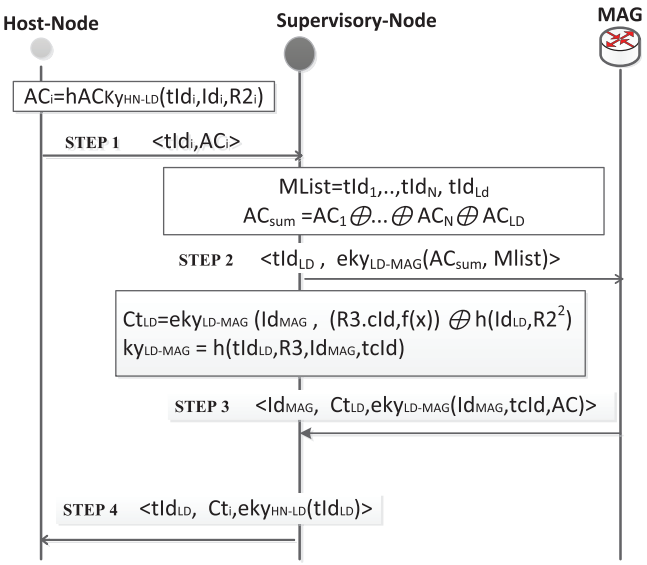

Figure 4: Initial-authentication procedure of host-node or a cluster of host-nodes with the MAG in CBAS

Step 3: Upon receiving the RS message, MAG generates a random number R3. The function for pairwise keys (established between each group member and their group leaders) $f(x) = \sum_{i=1}^{N}(Ky_{i-LD} \prod_{1 \le j \le N, j \ne i} \frac{x - tId_j}{tId_i - tId_j}$ is used to computes the ciphertext (Ct_{LD}) and sends it to the

[5] HN refers to Host-Node, while LD refers to Supervisory-Node/leader.

Host-Node in a router advertisement (RA) message. When the Host-Node receives the RA message, it first decrypts Ct_{LD} using key (Ky_{LD-MAG} = h (tId_{LD}, R3, Id_{MAG}, tgId). Now Host-Node is able to obtain the random numbers R3 from the ciphertext.

Step 4: Then, the message <tId_{LD}, Ct_i, eKy_{HN-LD} (tId_{LD})> is forwarded to the Host-Node. The function f(x) is used for establishing the pairwise keys with each group member. The f(x) function value is stored in its memory. On receiving the authentication response from the Supervisory-Node, host-node decrypts the ciphertext using the session key $Ky_{HN\text{-}LD}$.

3.4 Handover Procedure

Several proposed authentication schemes [17–21] require that the authentication procedure is performed each time when a Host-Node attaches to a new base station. This results in a longer handover latency and heavy workload on the base station. In contrast, our proposed CBAS scheme supports a group handover authentication. It makes the authentication process not only fast but also leads to a shorter handover delay. The handover procedure is depicted in Fig. 5. When a Host-Node or group of Host-Nodes moves from the previous MAG (MAG_1) to the new MAG (MAG_2), handover occurs and following procedure is carried out:

Step 1: When a Supervisory-Node detects that a Host-Node or group of Host-Nodes have left their cluster, it sends a deregistration message to the previous MAG (MAG_1) and starts to transfer data stored in MAG_1 to the MAG_2. This information is required to attach all Host-Nodes to the MAG_2 through their Supervisory-Node.

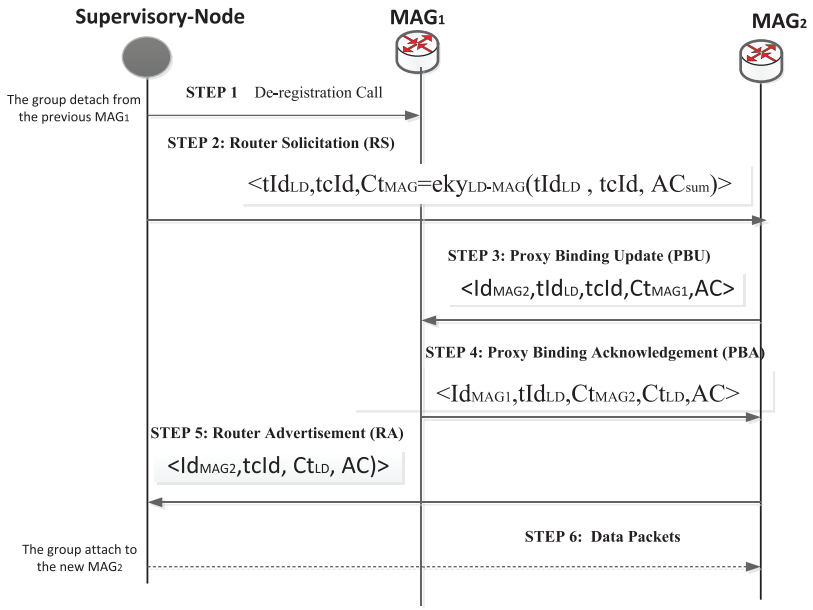

Figure 5: Handover procedure of host-node or a cluster of host-nodes from the MAG_1 to the MAG_2 in CBAS

Step 2: Before entering the domain of an MAG_2, the respective Supervisory-Node needs to collect the handover information of each Host-Node of its cluster, then it accumulates the information and then sends RS message to MAG_2.

Step3: After receiving a RS message, MAG_2 searches for a matched entry of a group of Host-Nodes in its MAG-table. In case of not finding any entry information, MAG_2 sends a proxy binding update (PBU) request to MAG_1 to update the Binding entry of Host-Nodes. PBU is a request message sent by a MAG for updating the binding of Host-Node for its current address.

Step 4: Then MAG_1 replies through proxy binding acknowledgement (PBA) message to MAG_2. PBA is an acknowledgement message sent by a MAG of updating the binding information of Host-Node.

Step 5: Once MAG_2 receives PBA, it creates entries for Host-Nodes and replies through the Router advertisement (RA) message and sends to the requesting Supervisory-Nodes.

Step 6: Then, Supervisory-Nodes re-organizes the buffered data packets and transfers them to MAG_2. The group of Host-Nodes now successfully attached to the MAG_2.

4 Performance Evaluation

This section evaluates the proposed CBAS scheme by comparing it with SGMS [20] and LAMS [21] for 6LoWPAN. SGMS is a "secure group mobility scheme" to authenticate multiple 6LoWPAN resource constrained devices based on PMIPv6 (Proxy Mobile IPv6). LAMS is a lightweight authentication scheme to authenticate resource-constrained industrial devices by combining LMA functionalities with MAG in a 6LoWPAN gateway. All schemes are analyzed and compared based on the handover authentication delay and signaling cost analysis, which are considered key performance metrics. Tab. 2 summarizes the notations used in the analysis.

Table 2: Parameters used for Numerical Analysis [24,25]

Parameters	Description	Values
P_c	Control packets	50 bytes
P_d	Data packets	1000 bytes
a_{wl}	Bandwidth (wireless)	11 Mbps
d_{wl}	Delay(wireless)	10 ms
a_w	Bandwidth(wired)	100 Mbps
d_w	Delay(wired)	2 ms
H_{x-y}	Total hops between x and y	5
d_a	Average link delay	5 ms
f	Failure probability	0.5
M_g	Total gateways in network	20
u	Unit cost of binding update	3
v	Unit cost of lookup	2
j	Unit signaling cost of packet(wired)	2
k	Unit signaling cost of packet(wireless)	4
ρ	Inter-cluster Probability	0.5
M_{ah}	Total active hosts	200
T_s	Setup time	500 ms
N_{x-y}	Signaling cost of node N	2.5

4.1 Evaluation Metrices

Fig. 6 shows the network model that depicts the entities and their relationship in CBAS. In Eq. (1), $\boldsymbol{T_{x,y}(z)}$ shows the transmission delay of a Host-Node with size 'z'. Failure probability '*f*' can occur during the movement of Host-Node from x to y through wireless link. The transmission delay for a wireless link is expressed as:

$$T_{x,y}(z) = \frac{1}{(1-f) * \left(\frac{z}{a_{wl}} + d_{wl}\right)} \tag{1}$$

The Eq. (2) shows the transmission delay of a node with size 'z' when it travels from one gateway to another gateway connected via a wired link. $\boldsymbol{H_{x,y}}$ denotes the total hops between x and y. The transmission delay for wired link is expressed as:

$$T_{x,y}(z, H_{x,y}) = H_{x,y}\left(\frac{z}{a_w} + d_w + d_a\right) \tag{2}$$

The Signaling Cost is derived for comparing the performance of proposed CBAS with the existing SGMS and LAMS schemes. Signaling Cost is calculated by adding the Binding Cost (BC) with Delivery Cost (DC) of packets.

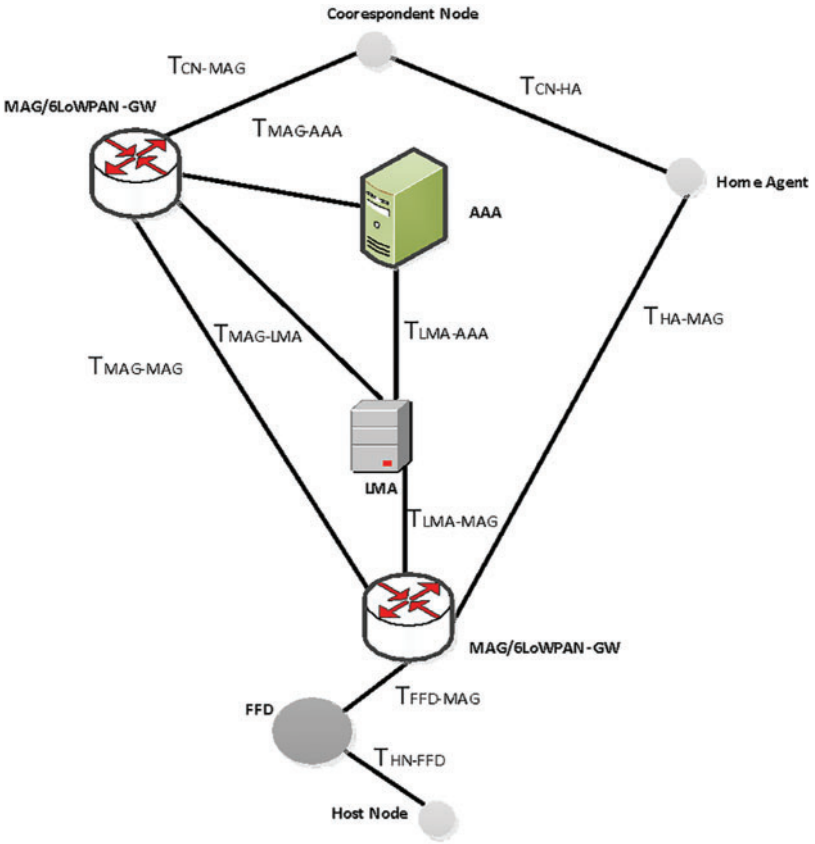

Figure 6: Network model

4.2 Analysis of Registration Delay

In this section, we will present the registration analysis of SGMS [20], LAMS [21], and our proposed scheme CBAS in 6LoWPAN.

4.2.1 Registration Delay of SGMS in 6LoWPAN

In SGMS scheme host node performs authentication request and reply operations with AAA server and exchanges PBU & PBA signals with LMA for registration of HN. After receiving the PBA message, the Router Advertisement message sends to MAG. The registration delay of SGMS is represented as:

$$RD_{SGMS} = 2T_{MN-LD}(P_c) + 2T_{LD-MAG}(P_c) + T_{MAG-LMA}(P_c, H_{MAG-LMA}) + 2T_{MAG-AAA}(P_c, H_{MAG-AAA}) \quad (3)$$

4.2.2 Registration Delay of LAMS in 6LoWPAN

In LAMS scheme, when a host node wants to register with a gateway (MAG/LMA), it sends Router Solicitation message. Then, gateway performs authentication request and reply operation with the AAA server. Based on the above scenario and Eq. (2), registration delay of LAMS is represented as:

$$RD_{LAMS} = 2T_{MN-LD}(P_c) + 2T_{LD-MAG}(P_c) + 2T_{MAG-AAA}(P_c, H_{MAG-AAA}) \quad (4)$$

4.2.3 Registration Delay of CBAS

In our proposed CBAS scheme, cluster-based communication is done through the Supervisory-node. During the deployment of host nodes across the network, each HN in a cluster must register itself with the MAG. The HN sends a message to the Supervisory-node FFD. Next, FFD generates a list of all attached nodes and sends it to the MAG through an RS message. After performing the authentication process, the MAG sends an RA message to the HN through its FFD. The registration Delay of proposed CBAS is expressed as:

$$RD_{CBAS} = 2T_{MN-LD}(P_c) + 2T_{LD-MAG}(P_c) \quad (5)$$

4.3 Analysis of Handover Authentication Delay

In this section, we conduct performance analysis by comparing the proposed scheme (CBAS) with SGMS [20] and LAMS [21]. Our analysis focuses on the handover authentication Delay and signaling cost. Handover Delay is defined as the transmission period when a Host-Node cannot receive packets from the previous base station or when a Host-Node receives the first packet from the new base station.

4.3.1 Handover Authentication Delay of SGMS in 6LoWPAN

In SGMS scheme, when a Host-Node wants to attach to a new MAG, it must exchange the authentication request and then send the reply signal to the AAA server. After that, it performs PBU and PBA operations with the LMA. The Authentication Delay of SGMS is written as:

$$AD_{SGMS} = 2T_{MN-LD}(P_c) + 2T_{LD-MAG}(P_c) + 2T_{MAG-LMA}(P_c, H_{MAG-LMA}) + 2T_{MAG-AAA}(P_c, H_{MAG-AAA}) + T_{MAG-LMA}(P_d, H_{MAG-LMA}) \quad (6)$$

4.3.2 Handover Authentication Delay of LAMS in 6LoWPAN

In the LAMS scheme, a Host-Node must attach itself with the gateway (MAG/LMA) and exchanges authentication request and reply messages with the AAA server. After the authentication process, gateways perform binding operations to establish a handover tunnel. The Authentication Delay of LAMS is given below:

$$AD_{LAMS} = 2T_{MN-LD}(P_c) + 2T_{LD-MAG}(P_c) + 2T_{MAG-AAA}(P_c, H_{MAG-AAA}) + 2T_{MAG-MAG}(P_c, H_{MAG-MAG}) + T_{MAG-MAG}(P_d, H_{MAG-MAG}) \quad (7)$$

4.3.3 Handover Authentication Delay of Proposed CBAS Approach

In the proposed CBAS scheme, the handover occurs when a Host-Node moves between two MAGs. Once (New MAG) MAG_2 receives packets from the Host-Node via their supervisory-Node through the RS message. Then, it performs the authentication process with PBU and performs PBA operations with MAG_1 for a cluster of nodes. Then MAG_2 sends a RA message to the Host-Node through their supervisory-Node. The Authentication Delay of CBAS is written as:

$$AD_{CBAS} = 2T_{MN-FFD}(P_c) + 2T_{FFD-MAG}(P_c) + 2T_{MAG-MAG}(P_c, H_{MAG-MAG}) + T_{MAG-MAG}(P_{d,} H_{MAG-MAG}) \quad (8)$$

4.4 Analysis of Signaling Cost

The signaling cost is calculated by adding the Binding Cost (BC) with the Delivery Cost (DC) of a packet. Next, we evaluate signaling cost for SGMS, LAMS and proposed CBAS.

4.4.1 Signaling Cost Analysis of SGMS in 6LoWPAN

In the SGMS scheme, T_s represents the setup time requires for the connection establishment and binding update process between the Host-Node with MAG. $2jN_{MAG-AAA} + 2jN_{LMA-AAA}$ represents the authentication operation. $2jN_{MAG-LMA} + uloglog(M_g + M_{ah})$ is needed for binding operation with the LMA. Accordingly, the BC_{SGMS} can be expressed as:

$$BC_{SGMS} = T_s + P_c + (2jN_{MAG-LMA} + 2jN_{MAG-AAA} + 2jN_{LMA-AAA}) + ulog(M_g + M_{ah}) \quad (9)$$

In the SGMS scheme, the packet delivery cost from the Host-Node to LMA through the MAG is represented as $kN_{MN-MAG} + 2jN_{MAG-LMA(kN_{MN-MAG}+2jN_{MAG-LMA}+2jN_{LMA-CN})}$. The cost of packet sends from LMA to the MAG is $(C_{MAG-LMA})$. The cost of searching entry for the corresponding nodes is $vloglog(M_g + M_{ah})$. The Delivery Cost can be written as:

$$DC_{SGMS} = P_d + (kN_{MN-MAG} + 2jN_{MAG-LMA} + 2jN_{LMA-CN}) + vlog(M_g + M_{ah}) \quad (10)$$

Therefore, the TC of SGMS can be expressed as:

$$SC_{SGMS} = BC_{SGMS} + DC_{SGMS} \quad (11)$$

4.4.2 Signaling Cost Analysis of LAMS in 6LoWPAN

In the LAMS scheme, the handover occurs between two gateways. The cost of connection established between the Host-Node and MAG is $T_{s,}$. The cost of exchanging the authentication and binding messages between two MAGs is represented as $(2jN_{MAG-AAA} + 2jN_{MAG-MAG})$. Thus, the Binding Cost of the LAMS is written as,

$$BC_{LAMS} = T_s + P_c + (2jN_{MAG-AAA} + 2jN_{MAG-MAG}) + ulog(M_g + M_{ah}) \quad (12)$$

The process of packet delivery in LAMS is done between two MAGs is written as:

$$DC_{LAMS} = P_d + \left(kN_{MN-MAG} + 2jN_{MAG-MAG} + kN_{MAG-CN}\right) + vlog\left(M_g + M_{ah}\right) \quad (13)$$

Therefore, SC of LAMS can be written as:

$$SC_{LAMS} = BC_{LAMS} + DC_{LAMS} \quad (14)$$

4.4.3 Signaling Cost Analysis of the Proposed CBAS

In the proposed CBAS, during the handover process, the MAG_1 exchanges the binding update messages with MAG_2 through the Supervisory-Node and is represented as $(2k\ N_{FFD-MAG} + 2tN_{MAG-MAG}$. The processing cost of MAG is $(2u\ log\ log\left(M_g + M_{ah}\right))$. Thus, binding cost for the CBAS can be written as:

$$BC_{CBAS} = T_s + P_c(2kN_{FFD-MAG} + 2tN_{MAG-MAG}) + 2ulog\left(M_g + M_{ah}\right) \quad (15)$$

$\left(N_{MN-FFD} * N_{FFD-MAG}\right)$ is a cost of receiving a packet from the Host-Node to the MAG via the Supervisory-Node. On receiving the packet, neighboring MAGs exchange the message that requires $P_d \times 2jN_{MAG-MAG}$. The cost of MAG is represented as $vlog\left(M_g + M_{ah}\right)$. Therefore, the Delivery Cost for the CBAS can be written as:

$$DC_{CBAS} = P_d + ((k\left(N_{MN-FFD} * N_{FFD-MAG}\right) + 2j\ N_{MAG-MAG} + kN_{MAG-CN}) + vlog\left(M_g + M_{ah}\right) \quad (16)$$

$$SC_{CBAS} = BC_{CBAS} + DC_{CBAS} \quad (17)$$

5 Simulation Results and Discussions

In this section, we discuss our simulation results. The equations presented in Section 3 are used as a performance criterion. First, we discuss our simulation environment, then detailed analysis on the obtained results is presented. The parameters and their corresponding values are given in Tab. 3.

Table 3: Simulation parameters

Parameters	Type	Values
UDP	Traffic type	CBR (Constant bitrate)
	Packet size	1000 bytes
IEEE 802.11	MAC bandwidth	2 Mb/s
	Base station coverage area	20 m
	Radio-propagation model	Two Ray Ground
	Topography area	670 m × 670 m
Wired link (rate/delay):	Between CN & MAG	2 ms
	Between MAG & MAG	2 ms
Antenna model	Antenna/OmniAntenna	–
Time	Simulation end	100 s

5.1 Simulation Setup

The simulation environment used for evaluating the proposed scheme CGM6 is Network Simulator version 2 (NS2). The National Institute of Standards and Technology (NIST) package based on PMIPv6 is used with simulation platform ns-2.29 (network simulator version 29) running on Ubuntu 17.10. A patch (nist-pmip6-6lowpan-ns_2.29-ubuntu12_i386.deb) which integrates 6LoWPAN and PMIPv6 is used for the simulation [27]. All simulations are done on an Intel machine with a 2.40 GHz Core i3-3110 and 4GB of RAM. The AWK scripting language in NS2 is used for text processing and extraction of tr (tracing) file. NAM (Network Animator) is used for the NS2.29 simulation [28]. Results are simulated by using Xgraph.

5.2 Registration Delay

Fig. 7 shows the impact of registration delay for SGMS, LAMS, and CBAS schemes in 6LoWPAN. We can observe from the figure that our proposed scheme CBAS shows better performance. The implication is that, during the registration process, both SGMS and LAMS schemes exchange extra signaling messages over a wireless link in 6LoWPAN. For instance, in SGMS scheme control signals are exchanged from MAG to LMA and AAA, and in LAMS scheme control signals are exchanged from MAG to AAA. While, in the CBAS scheme, the authentication and binding operations are performed within the MAG. This avoids signaling overhead during the registration process leading to better performance.

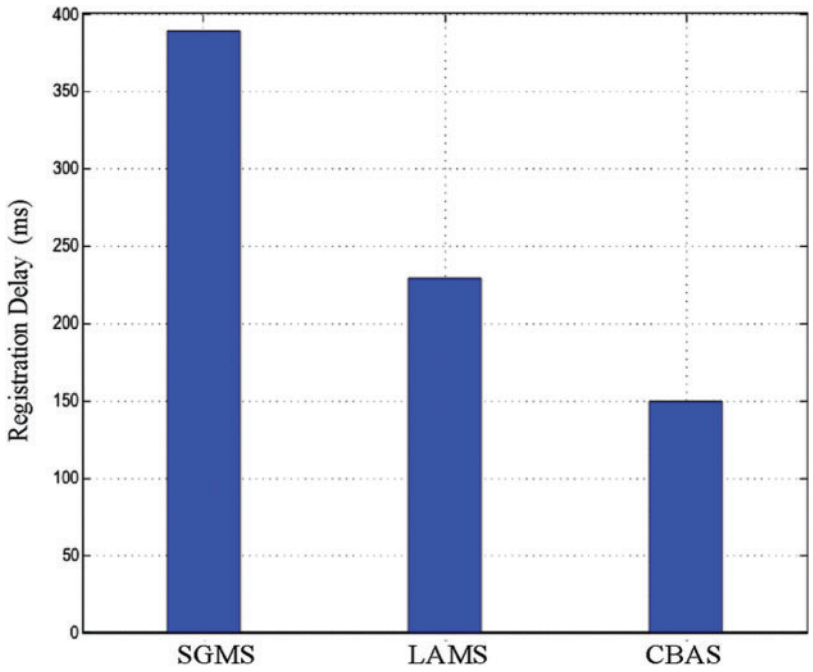

Figure 7: Effects of registration delay

5.3 Handover Authentication Delay

Fig. 8 shows the effects of the handover authentication Delay for the SGMS, LAMs, and CBAS schemes in 6LoWPAN. It can be observed from the figure that our proposed CBAS scheme performs better than SGMS and LAMS. The reason is that, in the CBAS scheme, authentication

and registration operations are combined in MAG. This avoids the extra signal exchange activities among the Host-Nodes in 6LoWPAN. It can also be observed from Fig. 7 that SGMS scheme shows the worst performance than LAMS and CBAS. This is due to the relief in LMA operations and integration of the authentication and binding operations in MAG. The implication is that the SGMS scheme consumes more time in processing than the two other schemes.

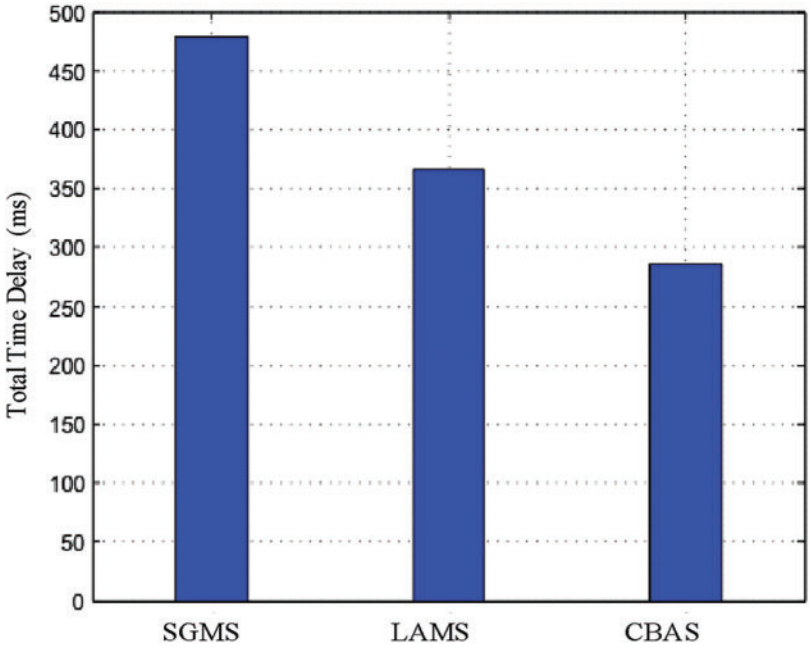

Figure 8: Effects of handover authentication delay

Figs. 9a and 9b shows the effects of wireless link delay (d_{wl}) and average queuing delay (d_a) on handover latency for SGMS, LAMS and CBAS schemes in 6LoWPAN. It can be observed from the figures that handover delay increases as wireless link delay and queuing delay increase. Our proposed CBAS scheme performs better than LAMS and SGMS. The reason is that, in CBAS scheme, group-authentication and binding operations are combined in MAG. This avoids the extra signal exchange activities among the nodes in 6LoWPAN.

5.4 Analysis of Signaling Cost

The effects of signaling cost is shown in Fig. 10. We can observe from the figure that, the signaling cost of the CBAS is lower than the LAMS and SGMS. This is due to performing the authentication process for a cluster of Host-Nodes via their Supervisory-Nodes, which further has reduced extra signaling messages among the entities of the CBAS.

6 Security Analysis

In this section, we provide the security analysis of CBAS, which is illustrated by low communication overhead and signaling cost, while attaining mutual authentication, device's identity confidentiality, and resistance against the following attacks: Modification attack, Replay attack, Man-in-the-middle attack and Impersonation attack.

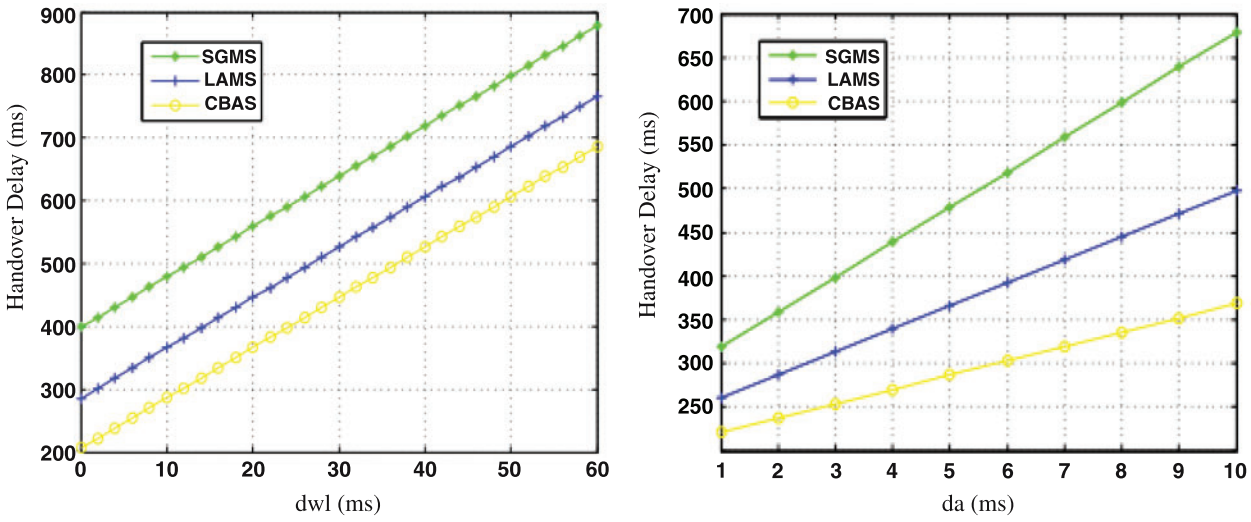

Figure 9: Effect of (a) Wireless link delay (d_{wl}) and (b) Average queuing delay (d_a) on handover

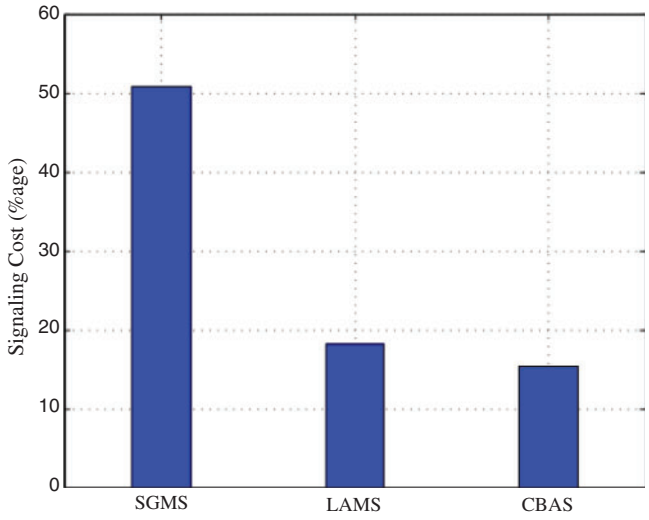

Figure 10: Effects of signaling cost

Proposition 1: Host-Node's identity confidentiality is provided by the CBAS scheme

Proof: In the proposed scheme, the Host-Node identity's confidentiality is based on the random number R1 and hash function $f(x) = \sum_{i=1}^{N}(Ky_{i-LD}\prod_{1\leq j\leq N, j\neq i}\frac{x-tId_j}{tId_i-tId_j}$ Since 'R1' is random number and difficult to guess by the intruder and hash function is non-reversible, the attacker cannot derive the host-node identity (Id_i) without knowing the random number and deriving the hash function. Furthermore, the Host-Node publishes the temporary identity (tId) to the public, and the actual identity is kept secret. It stops the attacker from accessing the Host-Node information and tracking the node.

Proposition 2: The proposed CBAS scheme provides entity mutual authentication

Proof. The proposed scheme provides mutual authentication between the Host-Node, Supervisory-Node and MAG because of the authentication code message (Msg). Upon receipt of the authentication code message (Msg), MAG checks and verifies the Host-Node legality by matching the Msg values with the received Msg value. The Host-Nodes cluster is considered valid if the equality holds. Otherwise, a warning message is sent to inform the cluster about the presence of the illegitimate node. Moreover, the adversary cannot generate the Msg value due to the lack of information about the R1 and R2(random numbers).

Proposition 3. The proposed CBAS resist to modification attack

Proof. To resist modification attacks, the proposed scheme uses random numbers (R1, R2 and R3) and a hash function h(), which makes it hard for an adversary to modify the information. The usage of random numbers and hash function guarantees that information cannot be modified without being detected.

Proposition 4. The proposed CBAS scheme provides protection against the replay attack

Proof. In the initial-authentication phase, a valid Host-Node sends an authentication code message (ACi = hACky$_{HN-LD}$ (tIdi, Idi, R2i)) to the MAG via its Supervisory-Node. If an attacker tries to impersonate the valid Host-Node by resending the previously obtained messages for extracting secret information, the MAG will not accept the authentication request. The reason is the Id of the Host-Node is based on a random number, which is only known to the valid Host-Node.

Proposition 5. The proposed CBAS provides protection against the Man-in-the-Middle attack

Proof. A man-in-the-middle-attack occurs when an unauthorized party intercepts the communication of two people/system. Moreover, two real/original parties assumed that they communicate directly with each other whereas they are interacting with the unauthorized party. In our CBAS approach, the *Msg* (Message authentication code) and hash function are used to prevent an adversary by launching a man-in-the-middle attack. However, if the attacker changes the ciphertext during communication, the receiver cannot decrypt it successfully using the right key. Thus, the illegal messages would be avoided.

Proposition 6. The proposed CBAS resist to Impersonation attack

Proof. An impersonation attack is a form of fraud to disguise as an authorized party by an attacker. In our proposed CBAS approach, all Host-Nodes must register with the MAG through the Supervisory-Node before the deployment. A Host-Node can be impersonated by the attacker, if the attacker hacks its confidential information such as random numbers. Otherwise, the MAG sends a warning message, when comparing the received information from attacker with the stored data in the MAG-Table and the information is unmatched. Moreover, the use of hash function in CBAS scheme also guarantees that information cannot be modified without being detected.

7 Conclusion

To resolve the authentication security issue of IP-based sensor nodes in 6LoWPAN, this paper proposed a cluster-based authentication scheme (CBAS) for highly constrained sensor nodes. The main goal of the proposed CBAS is to reduce the signaling cost during the handover and authentication procedures in 6LoWPAN and also ensure secure and efficient communication among the 6LoWPAN. In this approach, sensor nodes are organized into a cluster and communicate with the MAG through a cluster leader; we called Supervisory-Node. The Supervisory-Node communicates

with the MAG directly on behalf of the sensor nodes in the cluster. We also introduce a lightweight and efficient registration, de-registration, initial authentication and handover procedures when a sensor node joins or leaves a cluster. Our simulation experiments show that CBAS shows better performance in terms of low signaling cost during the registration and handover procedure compared to the state-of-the-art protocols. For instance, CBAS has reduced the registration delay by 11%, handoff authentication delay by 32%, and signaling cost by 37% compared to the state-of-the-art mobility management schemes. Our security analysis shows that the proposed CBAS approach protects against various security attacks, including Identity Confidentiality attack, Modification attack, Replay attack, Man-in-the-middle attack, and Impersonation attack.

Funding Statement: The authors would like to acknowledge the support of the Deputy for Research and Innovation, Ministry of Education, Kingdom of Saudi Arabia for this research through a Grant (NU/IFC/INT/01/008) under the institutional Funding Committee at Najran University, Kingdom of Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Ahmad, P. Laplante and J. F. DeFranco, "Life, IoT, and the pursuit of happiness," *IEEE Annals of the History of Computing*, vol. 22, no. 6, pp. 4–7, 2020.

[2] N. Anjum, Z. Yang, H. Saki, M. Kiran and M. Shikh-Bahaei, "Device-to-device (D2D) communication as a bootstrapping system in a wireless cellular network," *IEEE Access*, vol. 7, pp. 6661–6678, 2019.

[3] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally and M. A. Javed, "A survey of device-to-device communications: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2133–2168, 2018.

[4] N. Anjum, Z. Yang, I. Khan, M. Kiran, F. Wu *et al.,* "Efficient algorithms for cache-throughput analysis in cellular-D2D 5G networks," *Computers, Materials &Continua*, vol. 67, no. 2, pp. 1759–1780, 2021.

[5] D. Punia and R. Kumar, "Effect of mobility in IoT environment," in *2nd Int. Conf. on Trends in Electronics and Informatics*, Tirunelveli, India, pp. 1534–1537, 2018.

[6] T. Theodorou and L. Mamatas, "SD-MIoT: A software-defined networking solution for mobile internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4604–4617, 2021.

[7] X. Wang, "Multicast for 6LoWPAN wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 5, pp. 3076–3083, 2015.

[8] R. Beniwal, K. Nikolova and G. Iliev, "Performance analysis of MM-speed routing protocol implemented in 6LoWPAN environment," in *IEEE Int. Black Sea Conf. on Communications and Networking*, Sochi, Russia, pp. 1–5, 2019.

[9] T. Gomes, F. Salgado, S. Pinto, J. Cabral and A. Tavares, "A 6LoWPAN accelerator for internet of things endpoint devices," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 371–377, 2018.

[10] B. R. Al-Kaseem, Y. Al-Dunainawi and H. S. Al-Raweshidy, "End-to-End delay enhancement in 6LoWPAN testbed using programmable network concepts," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3070–3086, 2019.

[11] X. Wang, "A Mobility frame for 6LoWPAN WSN," *IEEE Sensors Journal*, vol. 16, no. 8, pp. 2755–2762, 2016.

[12] R. V. Vasilev and A. M. Haka, "Enhanced simulation framework for realisation of mobility in 6LoWPAN wireless sensor networks," in *IEEE XXVIII Int. Scientific Conf. Electronics*, Sozopol, Bulgaria, pp. 1–4, 2019.

[13] B. Maha and R. Abderrezak, "A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology," *Computer Communications*, vol. 74, no. 12, pp. 3–1515, 2016.

[14] N. b. H. Kasah , A. H. b. M. Aman , Z. S. M. Attarbashi and Y. Fazea, "Investigation on 6LoWPAN data security for internet of things," in *2nd Int. Conf. on Computer and Information Sciences*, Sakaka, Saudi Arabia, pp. 1–5, 2020.

[15] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *Int. Conf. on Pervasive Computing*, Pune, India, pp. 1–6, 2015.

[16] S. Jayasree, R. Sushmita and B. D. Sipra, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, no. 6, pp. 102481–102500, 2020.

[17] Y. Qiu and M. Ma, "A mutual authentication and key establishment scheme for M2M communication in 6LoWPAN networks," *IEEE Transactions on Industrial Informatic*, vol. 12, no. 6, pp. 2074–2085, 2016.

[18] L. M. L. Oliveira, J. J. P. C. Rodrigues, A. F. de Sousa and V. M. Denisov, "Network admission control solution for 6LoWPAN networks based on symmetric key mechanisms," *IEEE Transaction on Industrial Informatics*, vol. 12, no. 6, pp. 2186–2195, 2016.

[19] L. Gao, L. Zhang, L. Feng and M. Maode, "An efficient secure authentication and key establishment scheme for M2M communication in 6LoWPAN in unattended scenarios," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1603–1621, 2020.

[20] Y. Qiu and M. Ma, "Secure group mobility support for 6LoWPAN networks," *IEEE Internet Of Things Journal*, vol. 5, no. 2, pp. 1131–1141, 2018.

[21] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez *et al.,* "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 288–296, 2019.

[22] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy mobile IPv6, IETF RFC 5213," (Accessed 12 March 2021), 2008. [Online]. Available: https://www.hjp.at/doc/rfc/rfc5213.html.

[23] S. Choi and S. Koh, "Use of proxy mobile IPv6 for mobility management in CoAP-based internet-of-things networks," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2284–2287, 2016.

[24] M. Gohar, J. Choi, S. Koh, K. Naseer and S. Jabbar, "Distributed mobility management in 6LoWPAN-based wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 10, pp. 240, 2015.

[25] K. Imran, N. Anjum, S. Mahfooz, M. Zubair and Y. Zhahoui *et al.,* "Cluster-based group mobility support for smart IoT," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 2329–2347,2021.

[26] F. Aurelien and C. Claude, "TinyRNG: A cryptographic random number generator for wireless sensors network nodes," in *5th Int. Symp. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WIOPT'07)*, Limassol, Cyprus, 2007.

[27] K. A. Remley, J. A. Gordon, A. E. Curtin, C. L. Holloway, M. T. Simons *et al.,* "Measurement challenges for 5G and beyond: An Update from the national institute of standards and technology," *IEEE Microwave Magazine*, vol. 18, no. 5, pp. 41–56, 2017.

[28] M. Aman, S. Mahfooz, M. Zubair, K. Imran and S. Khusro, "Tunnel-free distributed mobility management (DMM) support protocol for future mobile networks," *Electronics*, vol. 8, no. 12, pp. 1519, 2019.